Compass Security

[The ICT-Security Experts]

Smashing PLCs for Fun and Profit

[Beer Talk – Berlin – 17.02.2015]

Stephan Sekula

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Darf ich mich vorstellen?

Stephan Sekula

- Seit August 2013 bei Compass als IT-Security Analyst
- Werdegang: Studium der Informatik, tätig in der Forschung; nun Sammeln von Praxiserfahrung
- Kompetenzen
  - War Dialing
  - ICS Devices

Hobbies

- Kochen & Backen
- Fahrradfahren
- Klettern
- IT-Sicherheit

Einführung

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Automatisierung im Alltag

Fertigung

http://www.youtube.com/watch?v=Kpvr2MVZjws&feature=plcp

http://www.youtube.com/watch?v=YFbBVzYaH_E

Qualität
Produktivität

Prozesse

Bikinger, „Raffinerie Schwechat“, CC-Lizenz (BY 2.0)

Paul-Gerhard Koch, „Kaprun“Bikinger, CC-Lizenz (BY 2.0)

kritische Infrastruktur

Gebäude

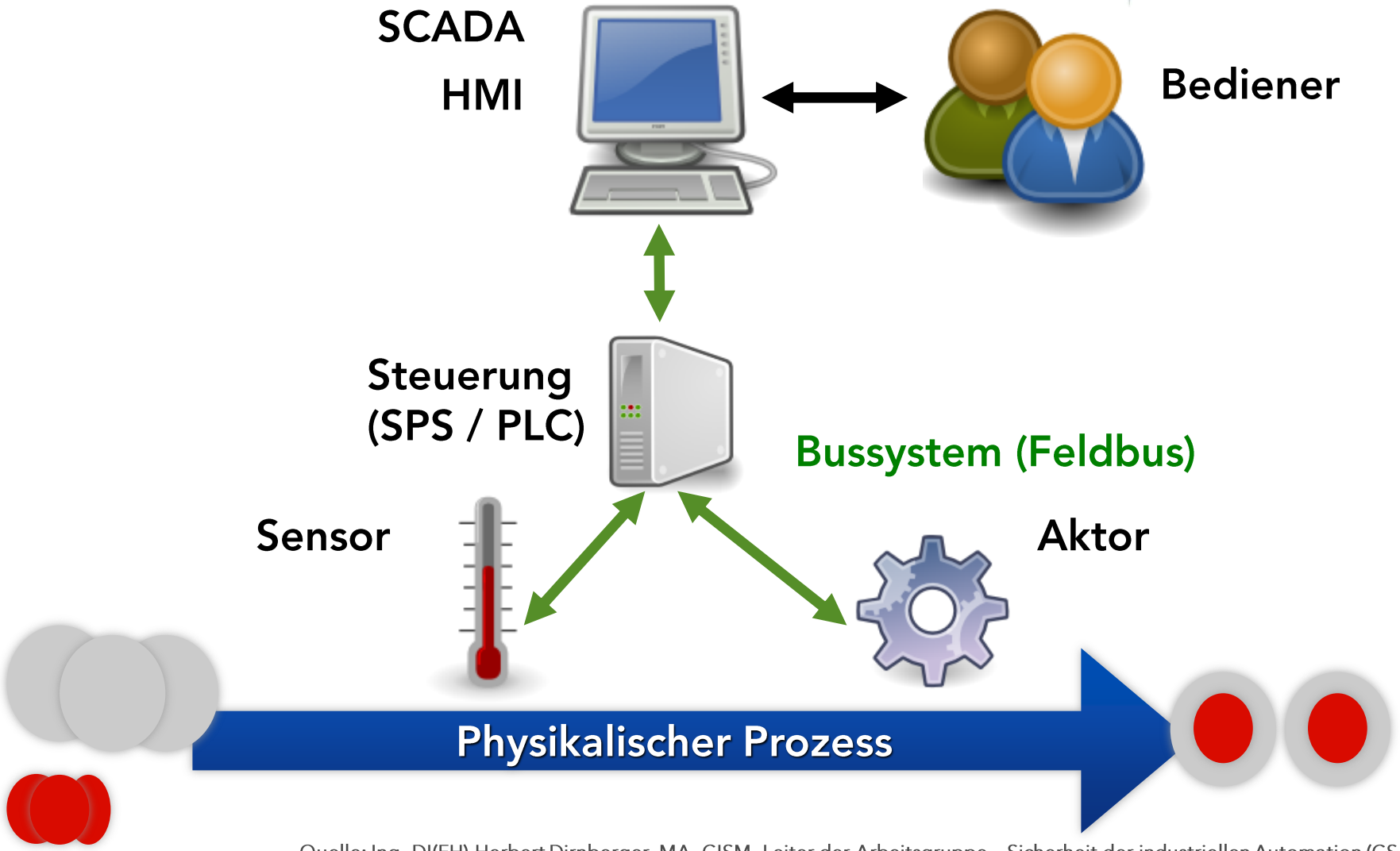
teakettle, „u1“, CC-Lizenz (BY 2.0)

SCADACS (IRAM) – FU Berlin (Prof. Dr.-Ing. Volker Roth)

Transport

Quelle: Ing. DI(FH) Herbert Dirnberger, MA, CISM- Leiter der Arbeitsgruppe – Sicherheit der industriellen Automation (CSA)

Automatisierung in 2 min.



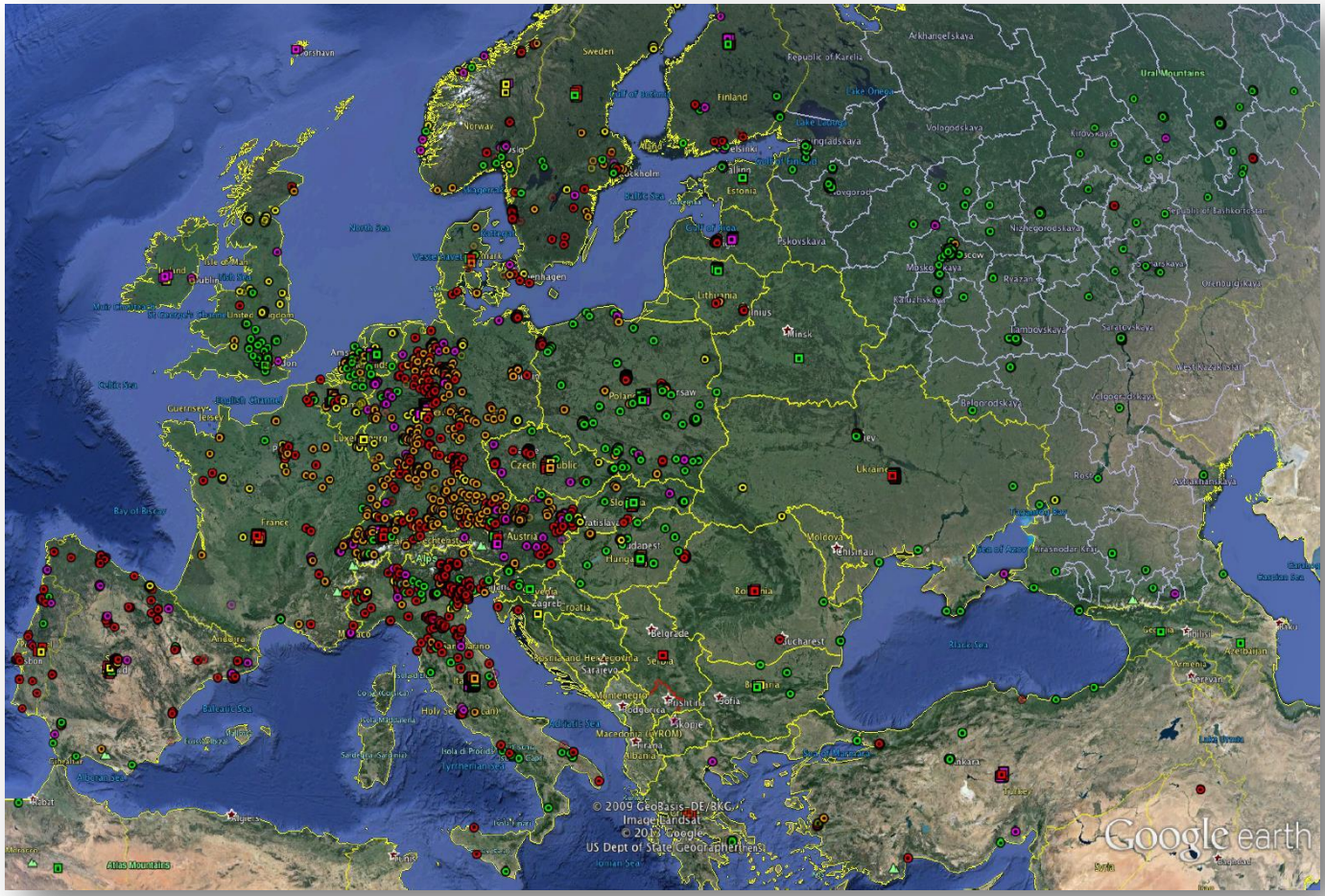
Quelle: Ing. DI(FH) Herbert Dirnberger, MA, CISM- Leiter der Arbeitsgruppe – Sicherheit der industriellen Automation (CSA)

Programmable Logic Controller (PLC)

Speicherprogrammierbare Steuerung (SPS)

Gute Gründe für Industrial Security

ICS Systeme in Europa – verwundbar (IRAM)



Quelle:
SCADACS (IRAM) – FU Berlin (Prof. Dr.-Ing. Volker Roth)

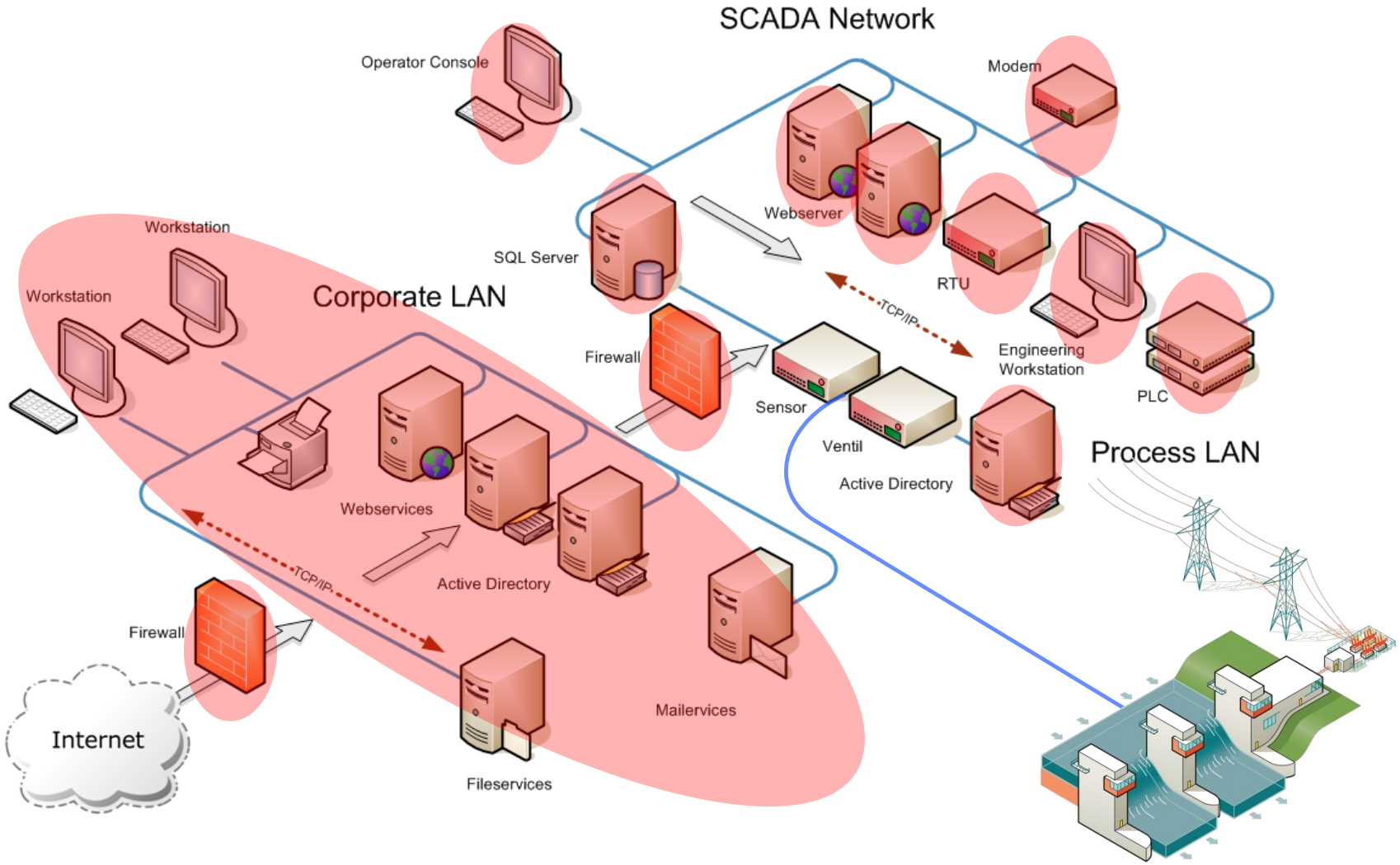
Angriffsflächen

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

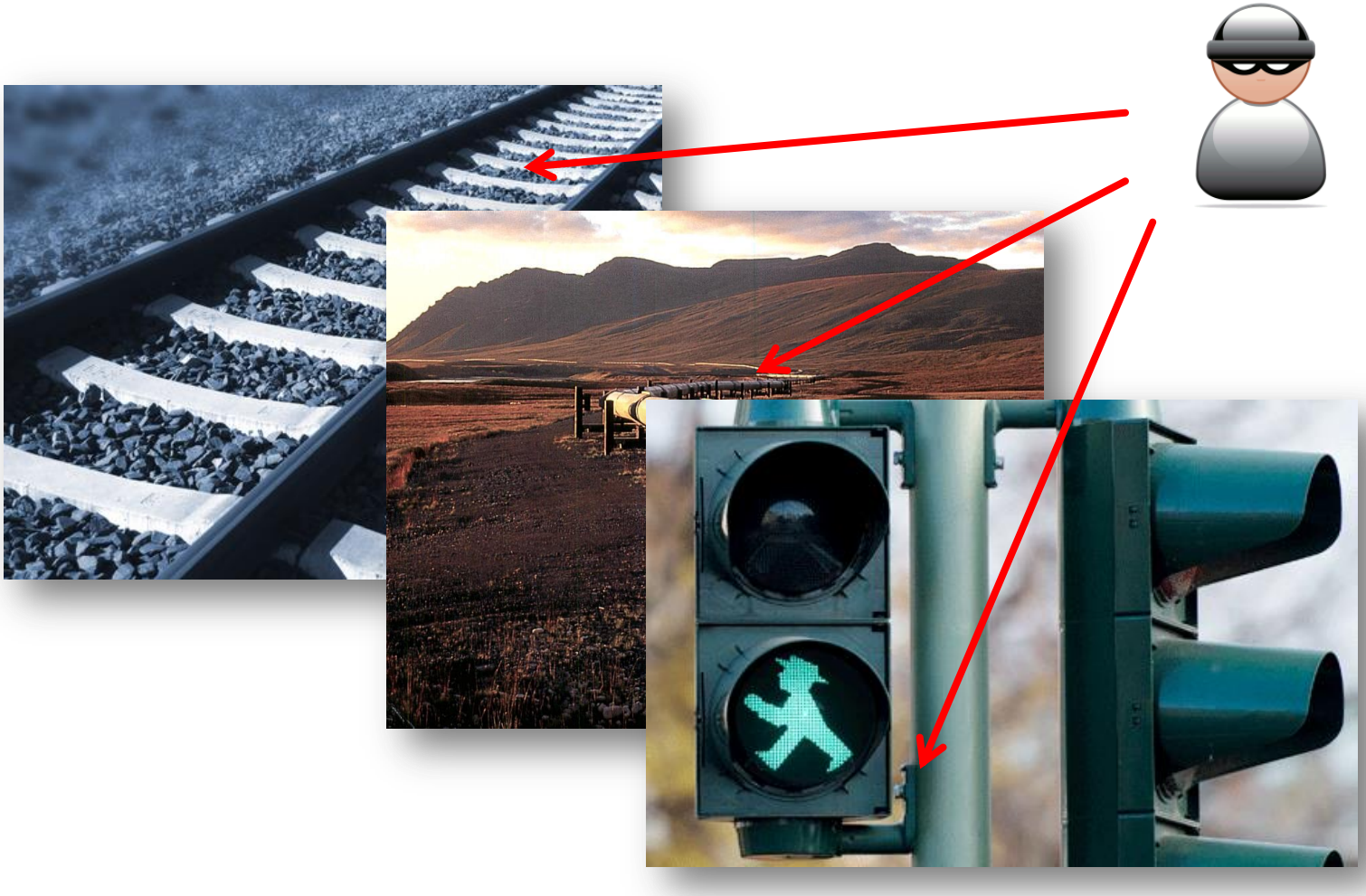
Industrial Network Architecture

Ansatzpunkte möglicher Angriffe



Industrial Network Architecture

The Real World...



Situation und Entwicklung

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

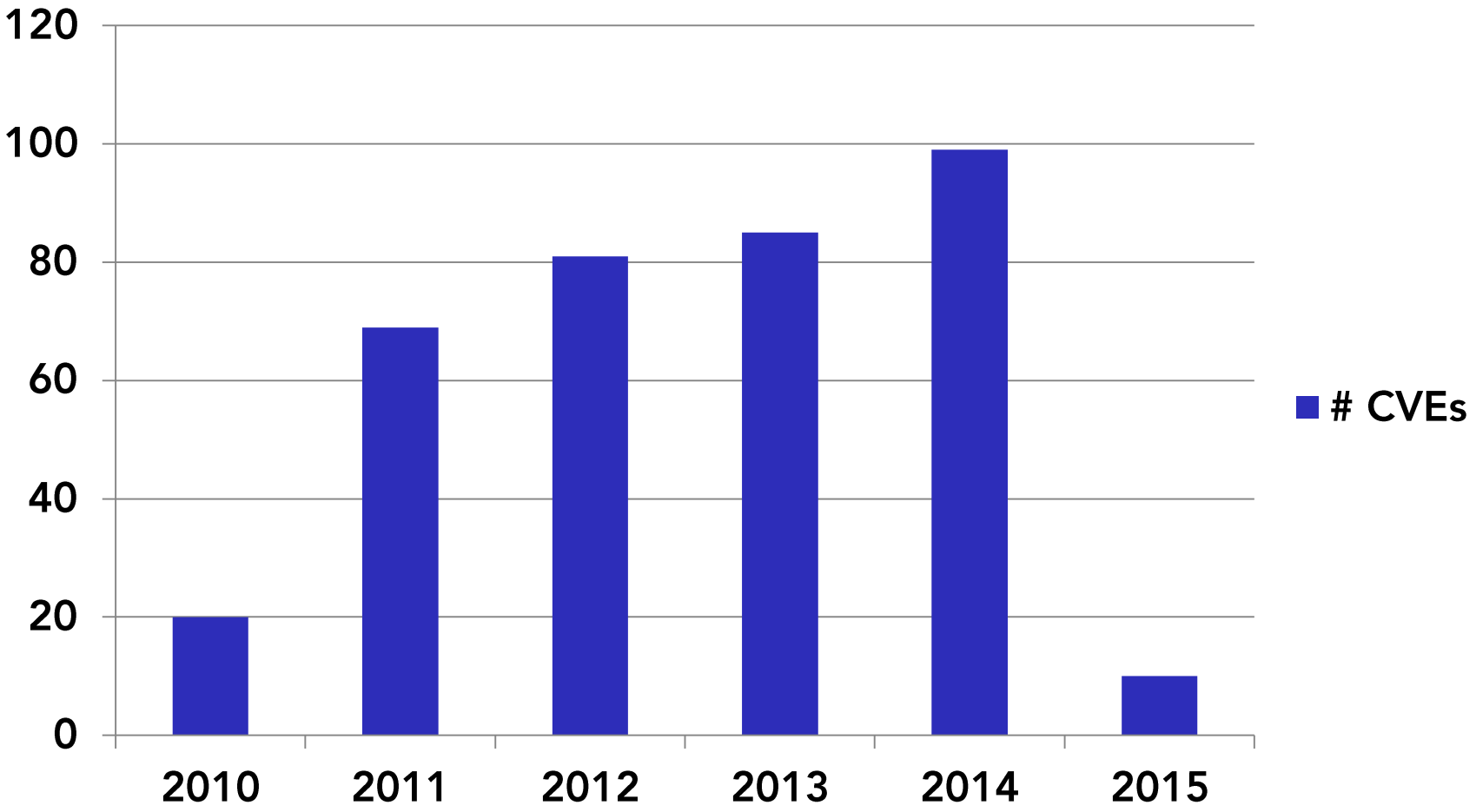
Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Herausforderungen

- Zunehmende Vernetzung
- Protokolle sind unzureichend gesichert
- Lange Lebenszeit der Systeme
- Systeme können oder werden nicht gepatcht

CVE Entwicklung

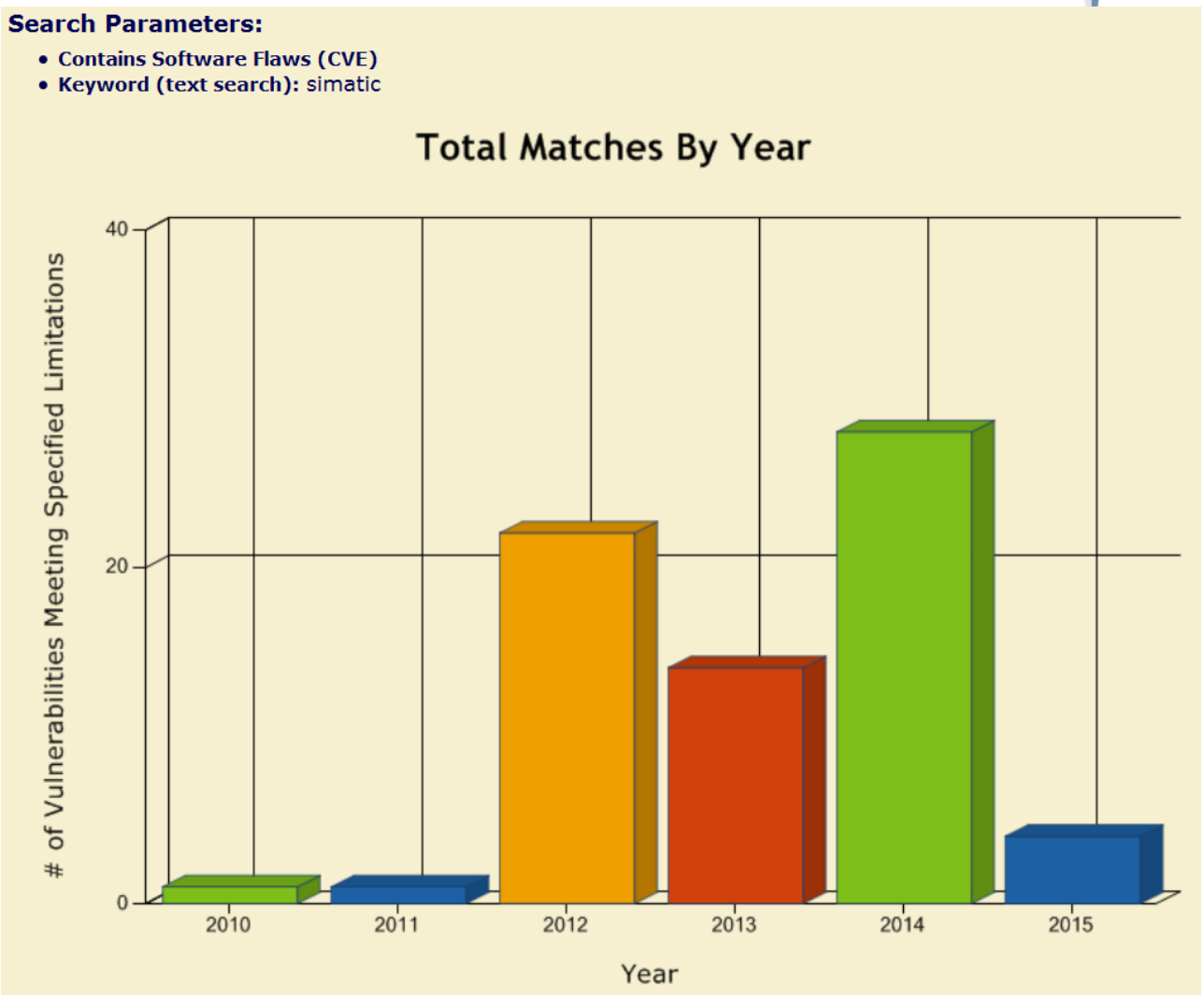
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM



CVE Entwicklung

Search Parameters:

- **Contains Software Flaws (CVE)**
- **Keyword (text search):** simatic



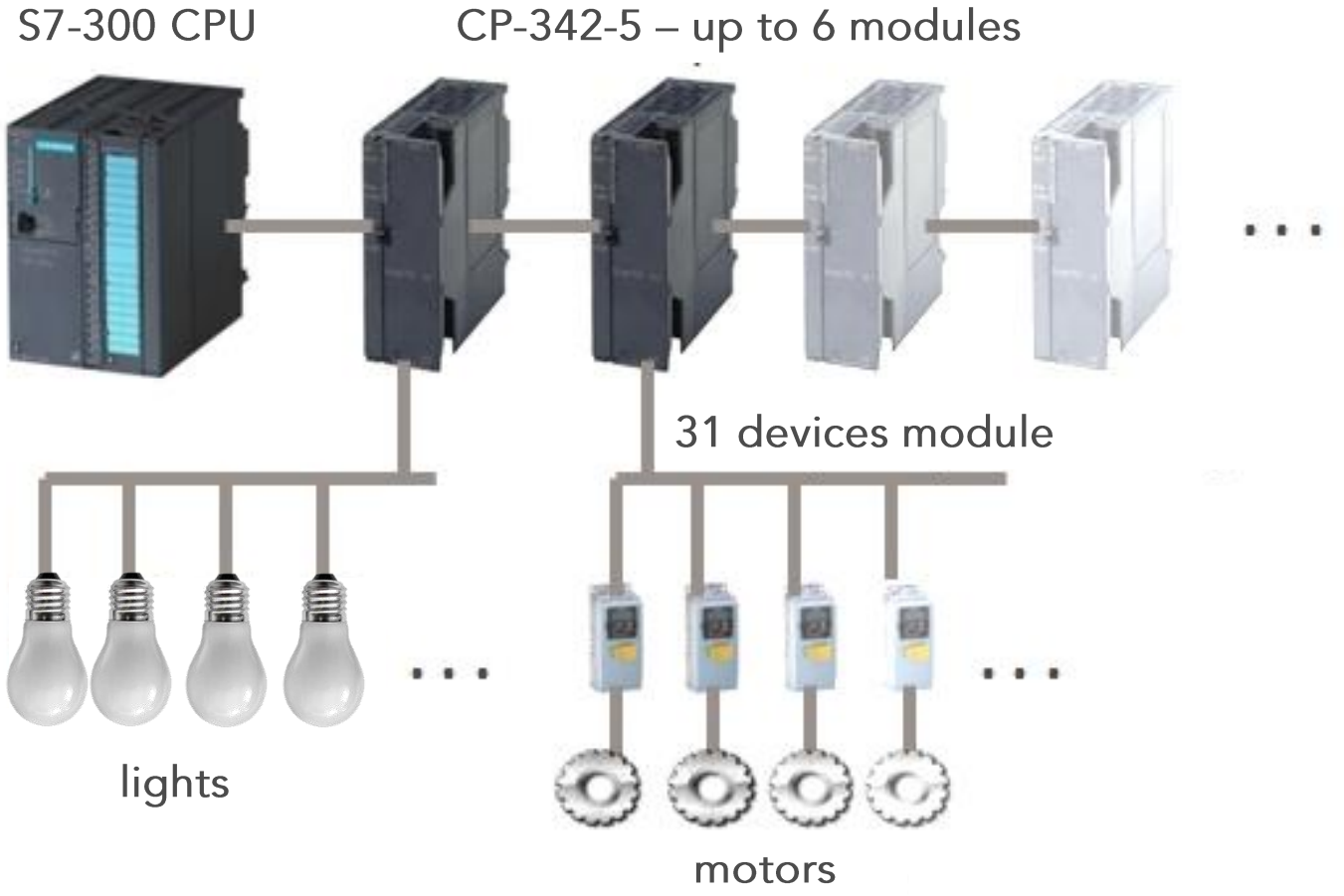
Quelle: https://web.nvd.nist.gov/view/vuln/statistics

LiveDemo
[Attacking Industrial Control Systems]

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

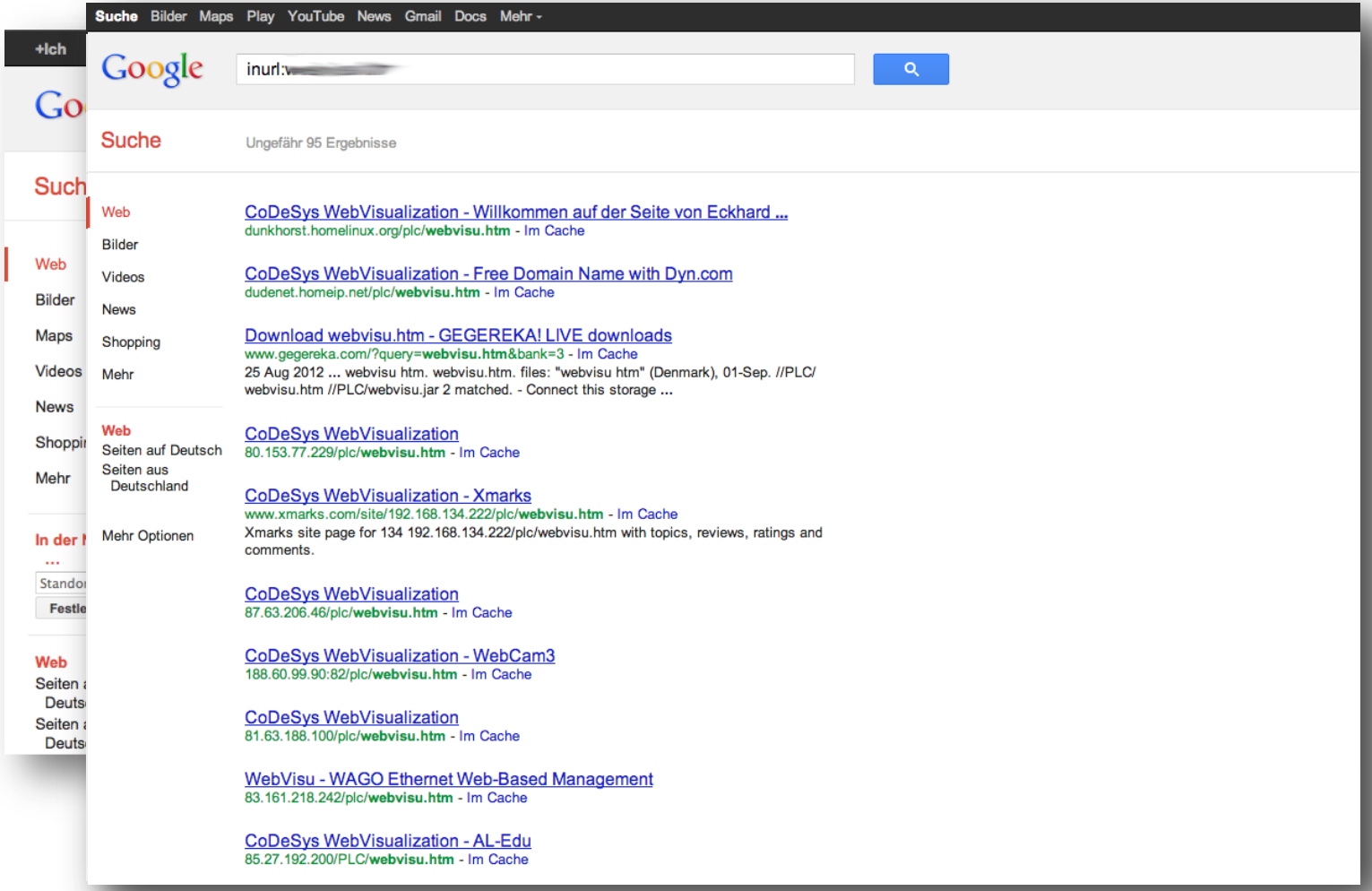
Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Simulationsaufbau



Gute Gründe für Industrial Security

Öffentlich zugängliche Systeme



Gute Gründe für Industrial Security

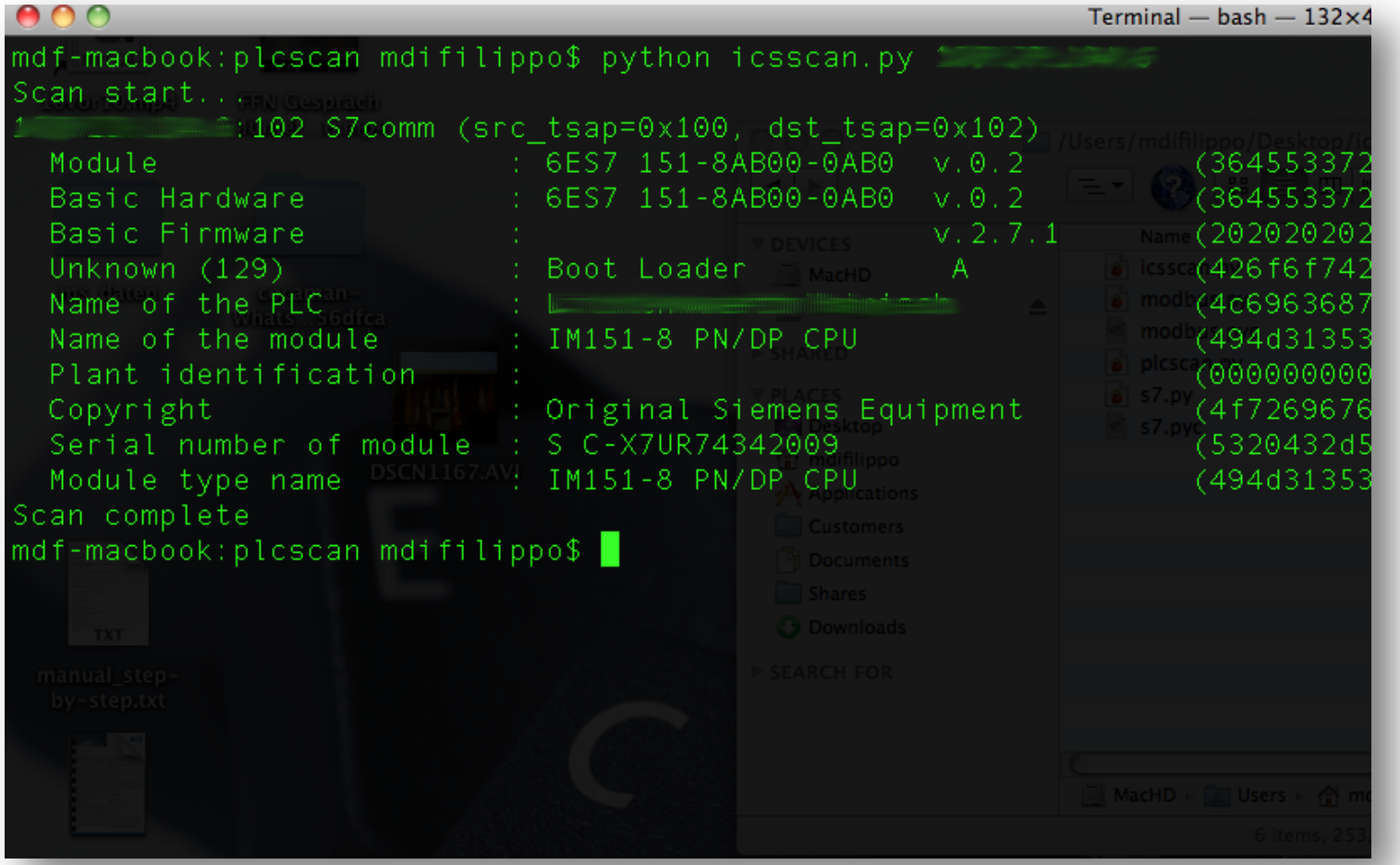
Öffentlich zugängliche Systeme

SHODAN
Computer Search Engine

82.55.34.62 Telecom Italia Added on 06.11.2012 Città Di Castello host62-34-dynamic.55-82-r.retail.telecomitalia.it	Inline controller with Ethernet interface for coupling to other controllers or systems, with programming in acc. IEC 61131-3
91.80.10.127 Vodafone Omnitel N.V. Added on 19.10.2012	Inline controller with GSM/GPRS interface for coupling to other systems, with programming in acc. with IEC 61131-3
31.61.112.227 PTK CENTERTEL mobile data services Added on 19.10.2012	Inline controller with Ethernet interface for coupling to other controllers or systems, with programming in acc. IEC 61131-3
85.44.179.2 Les Griffes Srl Added on 18.10.2012 host2-179-static.44-85-b.business.telecomitalia.it	Inline controller with Ethernet interface for coupling to other controllers or systems, with programming in acc. IEC 61131-3
188.171.255.249 Sociedad Promotora de las Telecomunicaciones en As Added on 18.10.2012	Inline controller with GSM/GPRS interface for coupling to other systems, with programming in acc. with IEC 61131-3
31.61.112.193 PTK CENTERTEL mobile data services Added on 18.10.2012	Inline controller with Ethernet interface for coupling to other controllers or systems, with programming in acc. IEC 61131-3
92.48.157.247 Proximus Mobile Internet Added on 03.10.2012	Inline controller with GSM/GPRS interface for coupling to other systems, with programming in acc. with IEC 61131-3

Gute Gründe für Industrial Security

Öffentlich zugängliche Systeme

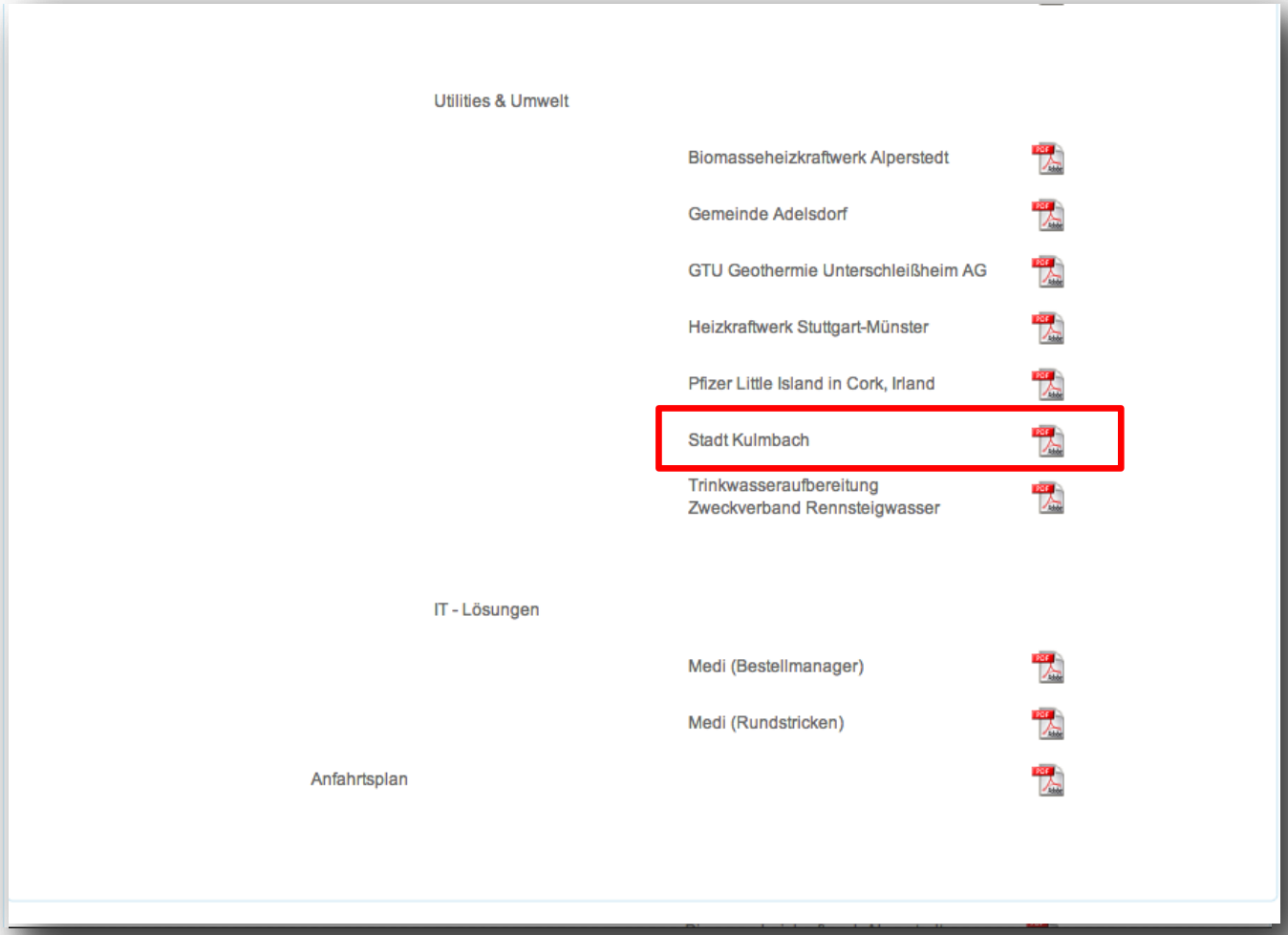


Gute Gründe für Industrial Security

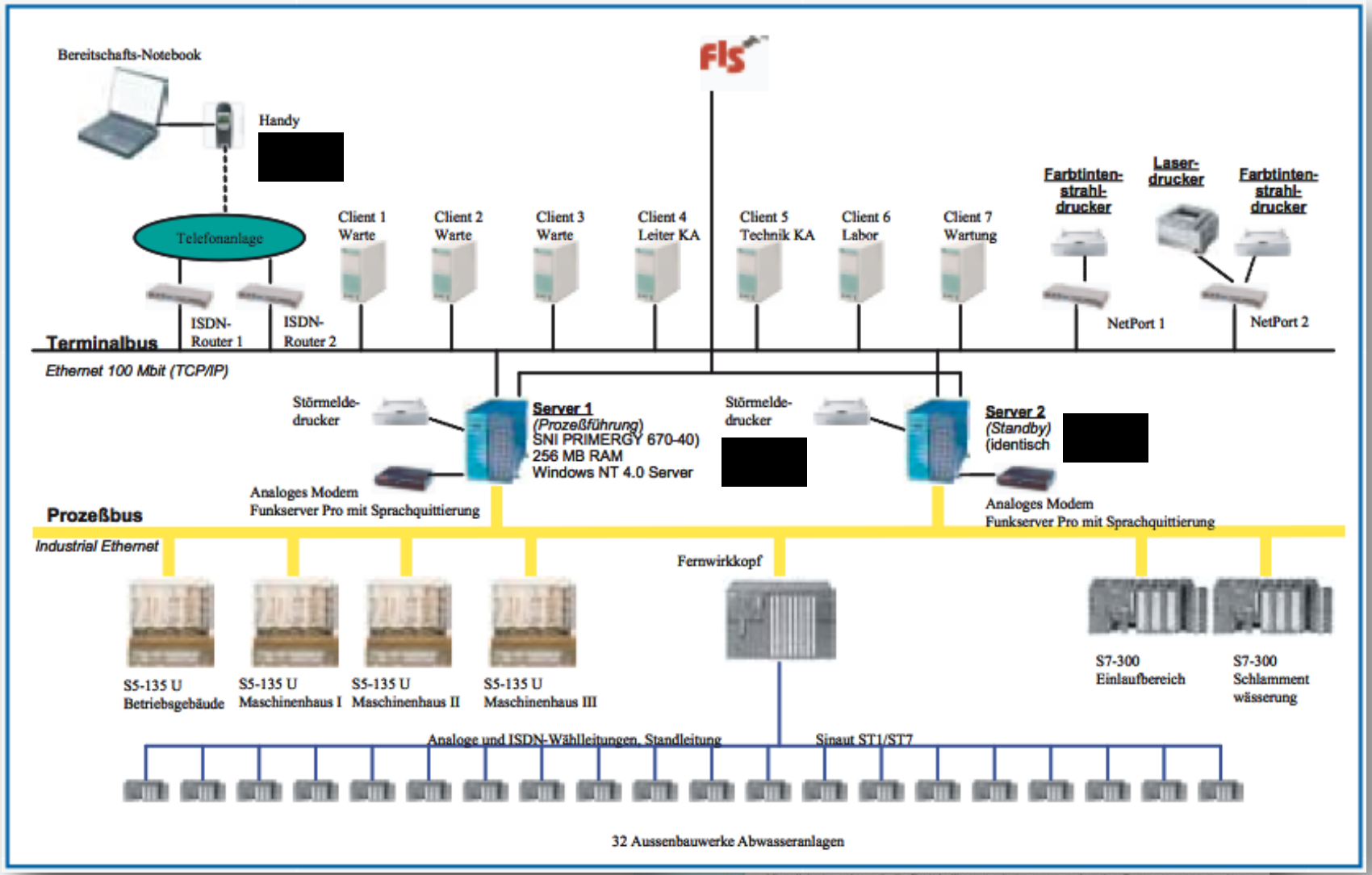
Beispiele

WarGoogling 2.0

Noch einfacher....



WarGoogling 2.0



Trunk-Scanning [WarDialing]

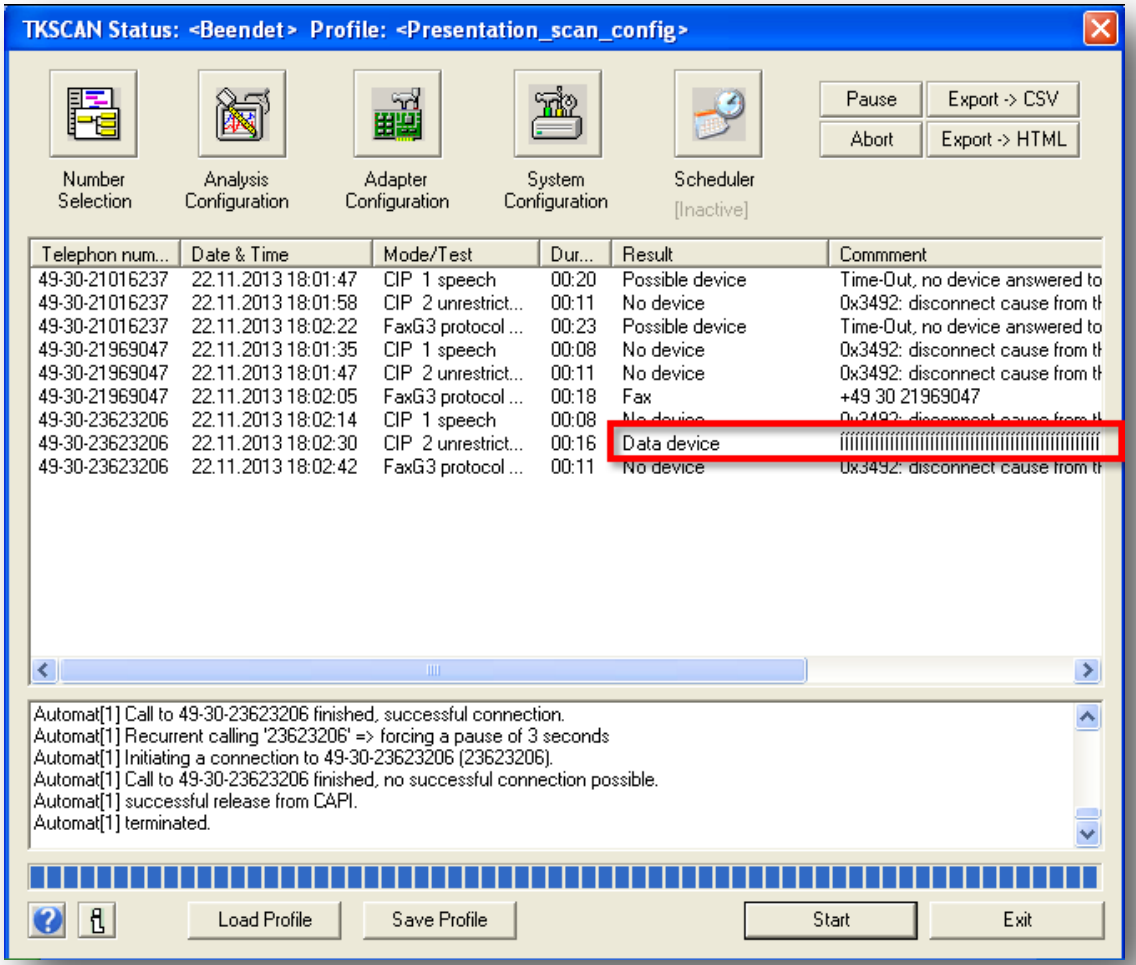
Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Ziele des WarDialing

- Identifikation des Nebenstellentyps (Sprache, Modem, FAX, ISDN Daten).
- Erkennung von Modems, Fernwartungszugängen, Einwahlsystemen, Anrufbeantwortern und FAX Servern.
- Potentiell verwundbare Systeme werden weiter analysiert.

WarDialing


TKSCAN Status: <Beendet> Profile: <Presentation_scan_config>
Number Selection
Analysis Configuration
Adapter Configuration
System Configuration
Scheduler
[Inactive]
Pause
Export -> CSV
Abort
Export -> HTML
Telephon num...
Date & Time
Mode/Test
Dur...
Result
Commment
49-30-21016237 22.11.2013 18:01:47 CIP 1 speech 00:20 Possible device Time-Out, no device answered to
49-30-21016237 22.11.2013 18:01:58 CIP 2 unrestrict... 00:11 No device 0x3492: disconnect cause from th
49-30-21016237 22.11.2013 18:02:22 FaxG3 protocol ... 00:23 Possible device Time-Out, no device answered to
49-30-21969047 22.11.2013 18:01:35 CIP 1 speech 00:08 No device 0x3492: disconnect cause from th
49-30-21969047 22.11.2013 18:01:47 CIP 2 unrestrict... 00:11 No device 0x3492: disconnect cause from th
49-30-21969047 22.11.2013 18:02:05 FaxG3 protocol ... 00:18 Fax +49 30 21969047
49-30-23623206 22.11.2013 18:02:14 CIP 1 speech 00:08
49-30-23623206 22.11.2013 18:02:30 CIP 2 unrestrict... 00:16 Data device
49-30-23623206 22.11.2013 18:02:42 FaxG3 protocol ... 00:11 No device
Automat[1] Call to 49-30-23623206 finished, successful connection.
Automat[1] Recurrent calling '23623206' => forcing a pause of 3 seconds
Automat[1] Initiating a connection to 49-30-23623206 (23623206).
Automat[1] Call to 49-30-23623206 finished, no successful connection possible.
Automat[1] successful release from CAPI.
Automat[1] terminated.
Load Profile
Save Profile
Start
Exit

Shellshock

Quellen:
www.filoo.de/blog/wp-content/uploads/2014/09/shellshock.png
openclipart.org/image/800px/svg_to_png/202367/shellshock-bug.png

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Was ist Shellshock?

- Schwachstelle bestimmter Versionen der Bash Shell
- Befehle, die nach Funktionsdeklarationen in Umgebungsvariablen auftreten, werden ausgeführt:

```
$ env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

Funktions-deklaration

Sollte nicht ausgeführt werden (kann ein beliebiger Befehl sein)

CVEs:
CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187

Shellshock

- Einige SPS verwenden eine (verwundbare) Version der Bash Shell
- Problem:
  - ICS Systeme erhalten kaum Sicherheitsupdates…
  - …oder können nicht aktualisiert werden

Security Guidelines

- Keine unnötige Exponierung von ICS-Geräten ins Internet
- Einführung einer ICS-Sicherheitszone
- Fernwartung ausschließlich über VPN
- Security Audits von internen und externen Komponenten
- Risikomanagement und Self-Assessment
- Schulung von Mitarbeitern

Wissen ist Macht...

- Wir wollen niemanden zu einer Straftat anstiften!
- Alle gezeigten Informationen dienen ausschließlich dazu, Sie zu sensibilisieren! Denn nur wer um die Gefahren weiß, kann sich davor schützen.
- Wenn Sie Fragen im Bereich IT-Sicherheit haben, sprechen Sie uns an.

Offene Diskussion

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

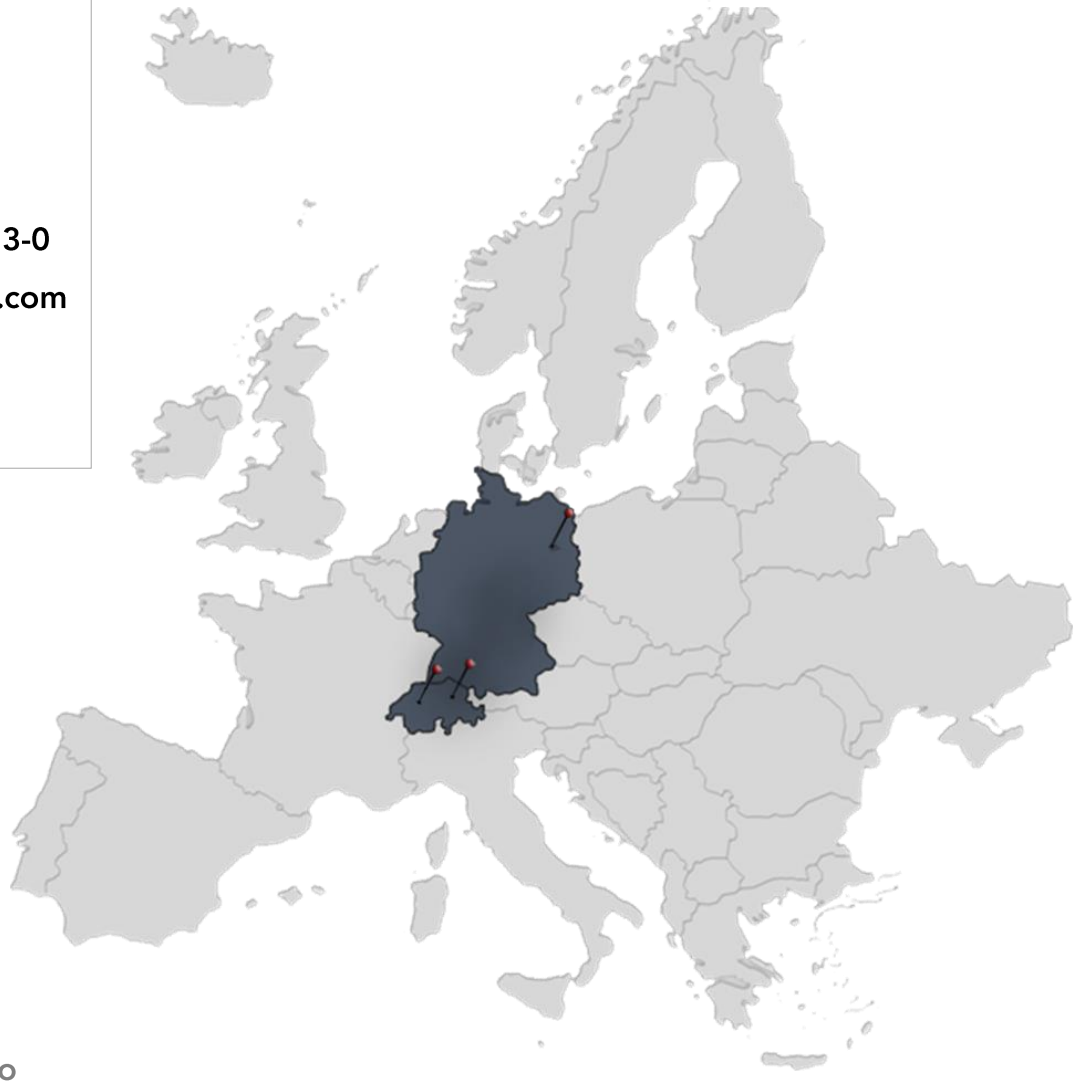
Compass Security Deutschland GmbH

Tauentzienstr. 18
10789 Berlin
Germany

team@csnc.de | www.csnc.de | +49 30 21 00 253-0

Secure File Exchange: www.filebox-solution.com

PGP-Fingerprint:
41CC 087A BF87 832F 7F0C 5FC3 CC36 7645 DAC0 B1EE



Slideconcept: Marco Di Filippo
Review: Laura-Louise Di Filippo